

REMARKS

The Examiner has deemed that the response filed 18 July 2003 was not fully responsive. The Examiner holds that (1) the Applicant gives no clear description of how content is decrypted; (2) or how it is used; (3) Applicant provides no clear connection to the content supplier, regarding claim 32) or the other elements of the other independent claims; (4) Applicant provides no support for the added claims; and (5) Applicant is required to show where amendments to the claims and the subject matter of the added claims is found in the original disclosure.

Regarding (1) and (2) above, the original specification states, for example, "Content supply unit 30 decrypts the encrypted key and key information by using co-owned key and stores the key and key information." Encryption and decryption using key information is well known in the art. See class 713 for example. That is, when data is encrypted using key information, it is necessary to that the decryption use the same key information used to encrypt data. The present invention is not directed to **how** the data is encrypted or decrypted, but is instead directed towards the **use** of encrypted data. One of ordinary skill in the art can use any known method to encrypt and decrypt the data. See the description with respect to fig. 4, for example of encryption/decryption process.

The original specification clearly describes the use of, for example, a **manufacturer key** encrypted for transmission and decrypted to be stored in a portable device (terminal). According to the original specification, MK_{PD} stands for the Manufacturer Key within a PD (personal device). Manufacturer Key, MK_{PD}, which is the pre-set manufacturer key in a temper {sic, tamper} resistant area within the PD, is to be used for the secure registration of a PD to LCM (Licensed Secure Digital

Music Initiative (SDMI) Compliant Module).

According to the original specification and as shown in Fig. 2, when a manufacturer request its registration to CA (Certificate Authority), CA certifies it and then generates a manufacturer key, MK_{PD} , and make its certificate data, $Cert_{CA}(ID_{MK})$, to deliver them to the manufacturer. At the same time CA generates a random token, T , to make (or update) the Manufacturer Key Information Table (MKIT) for the other ISP-registration. Once after a manufacturer got the data, $\{MK_{PD}, Cert_{CA}(ID_{MK})\}$, he/she can manufactures PDs by imbedding those secrete data within a tamper resistant area of PDs.

Accordingly, regarding (4) and (5) above, the forgoing clearly supports the claimed feature of *manufacturer key information embedded in said terminal* set forth in claim 32. As for the feature of *a symmetric key cryptosystem* note that with respect to the description of Fig. 4 of the original specification, ENC stands for symmetric Key Encryption of a content by utilizing a secret key. DEC stands for symmetric Key Decryption of a ciphertext by utilizing a secret key.

The specification also stated " CK_{PD-LCM} is a secure(secrete) channel key which is setup between PD and LCM. $EC_ENC(key, C)$ stands for an Elliptic Curve based Decryption of a ciphertext (encrypted text) C by utilizing a private key, key . $EC_DH(A, B)$ stands for a random secret value (key) shared between A and B by Elliptic Curve based Diffie-Hellman Key Exchanging Protocol. $ENC(key, C)$ stands for a Symmetric Key Encryption of a content C by utilizing a secrete key, key . *Samsung can support its own Symmetric Key Encryption algorithm, named "SNAKE", that is very effective for both S/W and H/W implementation and it has been world-wide cryptanalized.*

DEC(*key*, C) stands for a Symmetric Key Decryption of a ciphertext C by utilizing a secret key, *key*. Noting that in the above items the Elliptic Curve based Public Key Cryptosystem is just an example as a candidate of Public Key Cryptosystem, and so any public key cryptosystem, for example RSA, can be used instead of it."

Additionally, the original specification states, "Public Key Cryptosystem (PKC), such as ECC, RSA, ... (ECC is more preferable), is to be used for the secure key setup of LCM, the validity check of ISP's Public Key Certificate, and the secure channel construction between ISP and LCM. Symmetric Key Encryption Algorithm, such as SNAKE, is to be used for the content encryption, the authentication to a PD, and the secure channel construction between LCM and PD. Secure Chek-in/Chek-out System to be presented in section 6, 7 how to construct this system and how to securely maintain it."

As for the remaining features of claim 32, see the original specification section entitled "8. SECURE CONTENTS TRANSACTION RULE OVER ISP-LCM-PD-PM"

As for claim 33, the original specification states "For the LCM

Public Key Cryptosystem (PKC), such as ECC, RSA, ... (ECC is more preferable), is to be used for the secure key setup of LCM, the validity check of ISP's Public Key Certificate, and the secure channel construction between ISP and LCM. Symmetric Key Encryption Algorithm, such as SNAKE, is to be used for the content encryption, the authentication to a PD, and the secure channel construction between LCM and PD. Secure Chek-in/Chek-out System to be presented in section 6, 7 how to construct this system and how to securely maintain it.

For the PD

Public Key Cryptosystem (PKC) is an optional to PD. Symmetric Key Encryption Algorithm, such as SNAKE, is to be used for the content encryption, the authentication to a LCM, and the secure channel construction between PD and LCM. Manufacturer Key, MK_{PD} , which is the pre-set manufacturer key in a temper resistant area within the PD, is to be used for the secure registration of a PD to LCM."

It should be apparent from the foregoing information that the new claims and amended claims are supported by the original specification.

Regarding (3) above, claim 3 does not use the term "content supplier." However, it should be quite apparent, according to the specification, than when a user of the portable device (PD) wants to receive, for example, MP3 digital content data, the digital content is downloaded from the Internet service provider via a Licensed SDMI Compliant Module (LCM) such as a personal computer.

Accordingly, no new matter is added in the amendment filed 18 July 2003 and the amendments and newly added claims are supported by the original specification. Also note that the drawings may provide basis for the "written description" requirement of 35 USC §112, first paragraph. *Vas-Cath Inc. v. Mahurkar*, 19 USPQ2d 1111 (CAFC 1991) states:

"drawings alone may provide a "written description" of an invention as required by §112"; and *Ex parte Holt*, 19 USPQ2d 1211 (BdPatApp & Inter 1991) states:


"[the] invention claimed need not be described *ipsis verbis* in specification in order to satisfy disclosure requirement of 35 USC 112,.....since drawings in specification clearly illustrate...[the claimed invention]."

It is well established that the claims are to be read in light of the specification, see *In re Moore*, 169 USPQ 236 (CCPA 1971) and *In re Spiller*, 182 USPQ 614 (CCPA 1974), and as such the specification and drawings support the claimed invention.

The examiner is respectfully requested to reconsider the application, withdraw the objections and/or rejections and pass the application to issue in view of the above amendments and/or remarks.

A fee of \$420.00 is incurred by filing of a petition for two-month extension of time. Applicant's check drawn to the order of the Commissioner accompanies this Amendment. Should the check become lost or detached from the file, the Commissioner is authorized to charge Deposit Account No. 02-4943 and advise the undersigned attorney accordingly. Also, should the enclosed check be deemed to be deficient or excessive in payment, the Commissioner is authorized to charge or credit our deposit account and notify the undersigned attorney of any such transaction.

Respectfully submitted,


Robert E. Bushnell
Attorney for Applicant
Reg. No.: 27,774

1522 K Street, N.W.
Washington, D.C. 20005
(202) 638-5740
Folio: P55690
Date: 11/6/03
I.D.: REB/MDP